Amendments to the Specification

Please replace paragraph [0047] of the specification as published, with the following replacement paragraph:

[0047] Referring to FIG. 2, a method of computing a shared secret key is shown generally by the numeral 100. Alice selects an ephemeral private key x at random from the interval 1 to q-1 (102). Alice computes the corresponding ephemeral public key g^x and sends it to Bob (104). Similarly, Bob selects an ephemeral private key y at random from the interval 1 to q-1 (106). Bob computes the corresponding ephemeral public key g^y and sends it to Alice (108). Alice computes $s_A=(x + aR_A) \bmod q$ and the shared secret $K = R_B^{s_A} Y_B^{s_A R_B}$ (110) using simultaneous multiple exponentiation, as described below. Bob computes $s_B=(y + bR_B) \bmod q$ and the shared secret ~~$K = R_B^{s_A} Y_B^{s_A R_B}$~~ $K = R_A^{s_B} Y_A^{s_B R_A}$ (112) using simultaneous multiple exponentiation.